Bit-Tight Design: A Clean-Slate Approach to Hardware-Assisted Security and Resiliency

Ryan Kastner

Abstract: Hardware/software interfaces are riddled with holes (timing-channels, undefined instruction behaviors, storage-channels, memory access backdoors) through which secrets leak and attackers exploit. System designers are constantly forced to respond to these attacks, often only after significant damage has been inflicted. We propose a new hardware foundation for secure computing which will carefully and precisely manage all flows of information, making them explicit and verifiable from the hardware logic gates all the way up the system stack. This can be used to ensure private keys are never leaked (for secrecy), and that untrusted information will not used in the making of critical decisions (for safety and fault tolerance) nor in determining the schedule (real-time).

Biography: Ryan is currently a professor in the Department of Computer Science and Engineering at the University of California, San Diego. He received a PhD in Computer Science at UCLA, a masters degree (MS) in engineering and bachelor degrees (BS) in both Electrical Engineering and Computer Engineering, all from Northwestern University. He was born in Greensburg, PA and has spent his entire life moving westward - first to Medina, OH, then to Chicago, and finally California. His current research interests reside in the realm of embedded system design, in particular, the use of reconfigurable computing devices for digital signal processing.